Jelenkori társadalmi és gazdasági folyamatok, (2019) XIV. évfolyam, 3. szám, pp. 137–151.

INFORMATIKAI INFRASTRUKTÚRÁK BIZTONSÁGA A HAZAI EGÉSZSÉGÜGYI ELLÁTÁSBAN

Tisóczki József

Absztrakt: A biztonságot —különösen napjainkban — nem lehet egy egzakt kifejezéssel definiálni. A betegbiztonság egy „széles sávban" értelmezett komplex fogalom. A biztonságos betegellátás folyamatos biztosításához számos orvos-szakmai, műszaki-technológiai, energetikai, informatikai és logisztikai szakmaterület együttműködése szükséges. Ezek egyikének üzemzavara esetén már sérülhet a betegbiztonság. Jelen tanulmányomban egy rövid áttekintést adok a hazai egészségügyi ellátó-rendszer felépítéséről, kapcsolatrendszeréről. Ismertetem a létfontosságú rendszerelemek, mint fogalom létrejöttének indokoltságát, meghatározását, területeit és az alapokat adó főbb jogi szabályozókat. Különös tekintettel fókuszálok a kiemelten védendő kritikus infrastruktúrák (KIV) alá tartozó egészségügyi ellátó-rendszerek informatikai rendszereinek üzemeltetésére, annak folyamatosan változó kihívásaira.

Tanulmányom aktualitását adja az egyre nagyobb intenzitással megjelenő és mérhető kibertámadások gyakorlata, valamint a különleges adatoknak minősülő személyes egészségügyi adatok védelme. Megállapításom, hogy az egyén felelősségteljes informatikai infrastruktúra használata legalább akkora hatással van a biztonságos IT üzemre, közvetett módon a betegbiztonságra, mint a legkorszerűbb technológiák bevezetése és azok magas szintű használata.

Abstract: Security - especially nowadays - cannot be defined with an exact term. Patient safety is a complex concept interpreted as "broad band". In order to ensure safe patient care, there is a need for cooperation between a many medical-professional, technical, technological, energetic, IT and logistic areas. If one of these fails, patient safety may be damaged. In my study, I will give a brief overview of the structure and relationship system of the Hungarian health care system. I am focusing on the operation of IT systems for healthcare systems classified below critical infrastructure (CIS) to be protected, and on the ever-changing challenges.

The topicality of my study is the practice of cyber attacks that are becoming increasingly intense and measurable, as well as the protection of personal health data that qualify as special data. I find that using a responsible IT infrastructure has at least as much impact on secure IT operations, indirectly for patient safety, as the introduction of advanced technologies and their high use.

Kulcsszavak: kritikus infrastruktúrák, betegbiztonság, kiberbiztonság, egészségügyi informatika

Keywords: critical infrastructures, patient safety, cyber security, health informatics

1. Bevezetés

A kutatások az évek során egyre gazdagabbá tették az információ fogalmát, s helyét is kijelölték alapfogalmaink között. Az általánosítás legmagasabb fokán harmadik „princípiumként" az anyag és energia mellett jelölték ki a helyét, az élőlények létfenntartásában a táplálékkal és levegővel egyenrangú tényezőnek ismerték el, a gazdasági életben a nyersanyag, energia és munkaerő mellé, sőt fölé helyezték."… (Fülöp, 2001:8) Sokunk által ismert, napjainkra elcsépelt közhelynek tűnő mondat, mely szerint „az információ hatalom". Bármennyire is közhely, bizonyított módon igazságot hordozó kifejezés. A történelem során számos helyzet igazolta már. Ilyen volt például a Rotschild banking family információja, egy „értesülés" a waterlooi csata kimeneteléről. Ennek felhasználásával hatalmas vagyont hozott számukra a tőzsdén. Az információ hatalom, egyik ellenpéldája a World Trade Center 2001.

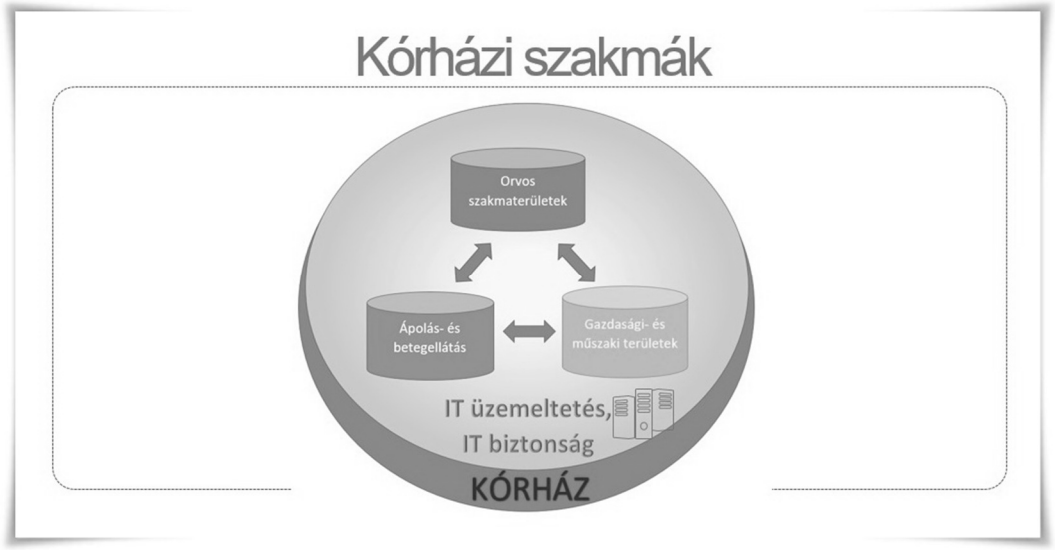
szeptember 11-i tragédiája, mikor is a korábbi jelzéseket figyelmen kívül hagyták az illetékesek. Az egészségügyi ellátásokhoz kapcsolódó információkra miként tekintsünk? Az egészségügyi informatika a betegellátási folyamatok támogatására szerveződött szolgáltatás, mely magában foglalja az ellátandókra és az ellátást végzőkre vonatkozó személyes adatok kezelését, a betegellátási folyamatok során keletkező adatok kezelését, ezen adatok felhasználásával történő kimutatások és jelentések készítését. E feladatok ellátását a non-stop üzem folyamatos biztosítása mellett, az aktuális jogszabályi környezethez igazodva, hardware és software környezet fenntartása és biztonságos üzemeltetése mellett kell, végezi. Bármely részelem sérülése, szolgáltatásának kiesése hatással lesz a betegellátásra, a betegbiztonságra. Ismertetem a főbb vonatkozó európai uniós és hazai jogszabályokat. Röviden kitérek az üzemeltetési feladatokat biztosító és az informatikai szolgáltatásokat igénybe vevő felhasználók érintettségére, figyelemmel az üzletmenetekre hatást gyakorló fenyegetettségekre is. Érintőlegesen szólok a hazai egészségügyi ellátásokhoz kapcsolódó informatikai infrastruktúra fejlesztésekről. Napjainkban egyre inkább az egyik legfőbb nemzetbiztonsági területté lép elő az információbiztonság. 2017 májusában a brit állami egészségügyi szolgálat (NHS) közleménye szerint 19 angliai körzetben, köztük London, Blackburn, Nottingham, Liverpool és Manchester egyes kórházaiban, de az internetes hírek szerint Nagy Britannia 40 különböző körzetében történt egészségügyi ellátórendszerek informatikai infrastruktúrái elleni célzott támadássorozat. Az érintett kórházak jelentős részében akadozott a telefonszolgáltatás és a számítógépes rendszerek működése. Ezekben a kórházakban a nem sürgősségi ellátást igénylő betegek fogadását felfüggesztették. Ebben az időszakban a Kasperky Lab biztonsági cég a WannaCry program jelentős aktivitását mérte a világ 74 országában, közel 45 ezer támadást észlelve. Bevezetőm zárásaként, mit is értünk biztonság, mint fogalom alatt? Amennyiben lehet egy fogalmat számtalan nézőpontból közelíteni és definiálni, —márpedig lehet és kell is— akkor e fogalommal ezt több tízszer megtették már. Dr. Virányi Gergely szerint a biztonság definíciója: „Eszme és megvalósítani remélt állapot” … „a biztonságban kiteljesedhet a természet, az egyén, a csoportok és az Emberiség léte.” (Virányi, 2012:15)

2. Alapvető fogalmak

Mikor egy rendszerről beszélünk, akkor egy egzakt módon behatárolt egységet értünk rendszer alatt, annak minden fizikai és virtuális alkotóelemével, entitásával együtt, ide értve a rendszerelemek közötti kapcsolódásokat és interakciókat, output szolgáltatásokat is. Infrastruktúra alatt definiált szabályok szerint több rendszer, interfészeken keresztül egymáshoz történő illesztését, azok együttes üzemét értjük. Kritikus infrastruktúrák azok az infrastruktúrák, amelyek bármilyen meghibásodása, esetleges megsemmisülése súlyos hatással van a nemzet vagy nemzetek biztonságára, a környezetre, a közegészségügyre, az állam, egyes kormányok hatékony működésére. Uniós tagállamként beszélhetünk Európai Uniós, illetve nemzeti létfontosságú rendszerelemről (LÉR) is. A LÉR, mint kifejezés hazai

fogalom, jelentésében, tartalmában is megegyezik a kritikus infrastruktúra kifejezéssel, melyet a 2012. évi CLXVI. törvény (Lrtv.) és a kapcsolódó 65/2013 (III. 8.) kormányrendelet vezetett be. Létfontosságú rendszerelem kifejezés alatt az Lrtv. 1-3. mellékletében meghatározott ágazatok valamelyikébe tartozó eszközt, létesítményt vagy egy rendszer olyan rendszer elemét értjük, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, melynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. Az egészségügyi ágazat is az Lrtv. alá sorolt ágazat. Nemzeti létfontosságú rendszerelem: az Lrtv. alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt jelentős hatást gyakorolna Magyarországra. Az egészségügyi informatika fogalmának meghatározásakor M.F. Collen definícióját idézem: „Az egészségügyi informatika a számítógépek, a kommunikáció, az informatika és az információs rendszerek alkalmazása az egészségügy minden területén. A betegellátásban, az egészségügyi képzésben, valamint az orvosi kutatásokban." (Morris F. Collen, 1986) Az egészségügyi informatika a kórházi ellátási folyamatok mindegyikében megjelenő, egyik részelem (lásd: *1. ábra*). Sérülése, szolgáltatásának kiesése esetén már sérülhet a betegbiztonság.

1. ábra: **Kórházi IT üzemeltetés kapcsolódási pontjai**



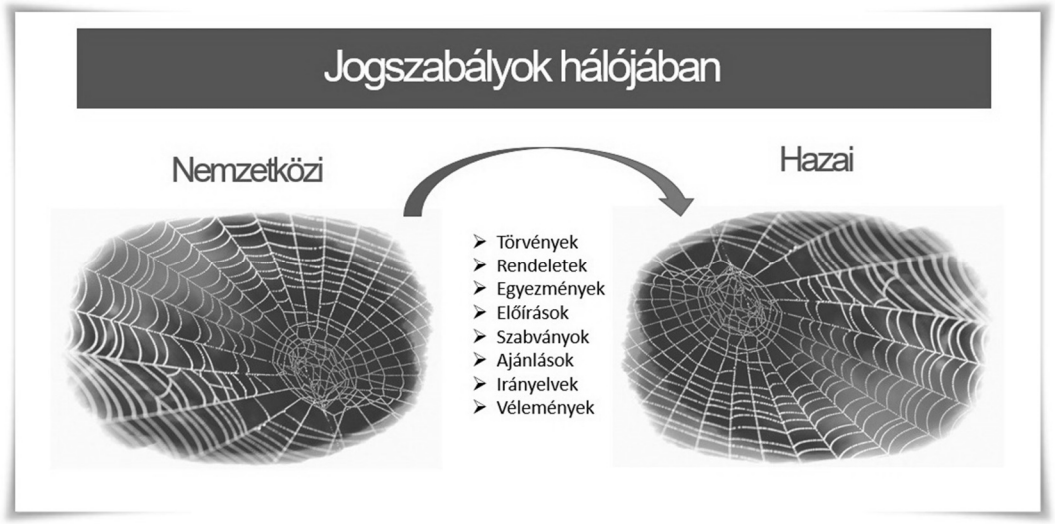
Forrás: A szerző saját szerkesztése. Tisóczki (2019)

3. Jogszabályi környezet

A digitális közszolgáltatások Magyarországon továbbra is a digitális gazdaság és társadalom legnagyobb kihívást jelentő területei közé tartoznak. Az EU országai közül Magyarország a 23. helyet foglalja el az adatok közigazgatási rendszerek közötti kezelésének területén. Ezt a 23. helyet foglalja el Magyarország a szolgáltatások kiépítettsége tekintetében is. 2017-ben az e-kormányzati szolgáltatások felhasználóinak aránya 45%-os volt. Ezzel szemben az uniós átlag

58% (European Unio, 2018). A jogszabályi környezet vizsgálatának kezdetét századunk indulásának időpontjában határoztam meg. 2001. szeptember 11-ét követően a terrorizmus elleni világméretű intézkedéssorozat újabb lökést adott a kibertér védelmét segítő jogi keretrendszerek kialakítására. Az USA Kongresszusa is ekkor fogadta el a Patriot Act-ot, melynek célja a jövőbeli terrorcselekmények megelőzése és kivédése volt (The USA Patriot Act, 2001). Vizsgálatomban fókuszáltam a hazai és nemzetközi jogi keretrendszerre, kísérletet tettem az aktuális jogi környezet feltérképezésére. Azokat a jogszabályokat, rendeleteket, ajánlásokat, határozatokat, szabványokat, kerestem, melyek valamilyen módon kapcsolódnak a hazai egészségügyi ellátáshoz. A jogi környezet adta szabályzók vizsgálatát követően hazai és nemzetközi viszonylatban egy rendkívül szövevényes kapcsolati hálót lehetne megrajzolni. A nemzetközi jogharmonizáció érdekében számos jogi aktus hazai megfeleltetése valósul meg (lásd: *2. ábra*).

2. ábra: **Nemzetközi jogi környezet hazai megfeleltetése**



Forrás: A szerző saját szerkesztése. Tisóczki (2019)

3.1. Európai uniós jogi aktusok

Az USA-ban bekövetkezett terrorcselekmények, az EU-t is érintő valós fenyegetettségek miatt az EU is megalkotta azt a jogi keretrendszert, mellyel rendezni kívánta a Kritikus Infrastruktúra Védelem (KIV) fenyegetettségeit, a kapcsolódó feladatokat, folyamatokat. Számos jogi aktus következett.

- 2004. június 17–18-án az Európai Tanács átfogó stratégia kidolgozására kérte fel a Bizottságot a létfontosságú infrastruktúrák védelmének javítása céljából. Válaszul a Bizottság 2004. október 20-án közleményt adott ki „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben” címmel (EUR-Lex 2018/1807, 2018) Ebben a stratégiában arra tettek javaslatokat, hogyan lehetne a megelőzés, felkészültség és reagáló képesség

európai dimenzióját javítani a kritikus infrastruktúrákat érintő terrortámadások esetén.

- 2005 november 17-én került sor a Zöld Könyv (EUR-Lex COM (2006) 786, (2007) kiadására, A létfontosságú infrastruktúrák védelmének európai programjáról. A Zöld Könyv elsődleges célkitűzése, hogy nagyszámú résztvevő bevonásával visszajelzéseket kapjon az EPCIP (European Programme for Critical Infrastructure Protection) lehetséges megközelítési irányairól. A létfontosságú infrastruktúrák hatékony védelme megköveteli valamennyi érintett fél – az infrastruktúrák tulajdonosai és üzemeltetői, a hatóságok, szakmai szervek és ágazati szövetségek – közötti kommunikációt, összehangolásukat és együttműködésüket nemzeti és uniós szinten egyaránt, úgy, hogy közben együttműködnek valamennyi kormányzati szinttel és a nyilvánossággal. A Zöld Könyv megfogalmazza, hogy a Bizottság hogyan kíván választ adni a Tanácsnak az EPCIP és a CIWIN (Critical Infrastructure Warning Information Network) felállítására vonatkozó felkérésére, mely a létfontosságú infrastruktúrák védelmére vonatkozó európai program kidolgozását célzó konzultációs eljárás második szakaszát képezi. A Bizottság a Zöld Könyv kiadásával remélte, hogy konkrét visszajelzéseket fog kapni az dokumentumban körvonalazott megközelítési lehetőségeket illetően.
- 2008 december 8. A Tanács 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (EUR-Lex COM(2005) 576, (2005). Az irányelv rendelkezik az ECI-k (Európai kritikus Infrastruktúrák) kijelöléséről, valamint meghatározza, hogy „Elsőbbséget kell biztosítani az IKT ágazatának." Rendelkezik még az 5. cikkben az Üzemeltetői biztonsági tervről, a 6. cikkben Biztonsági összekötő tisztviselő kijelöléséről, valamint jelentéstételi kötelezettségről, kapcsolattartó pontokról, felülvizsgálatról és végrehajtásról is.
- 2011. március 9-én került elfogadásra, Az Európai Parlament és a Tanács 2011/24/EU irányelve a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről. (EUR-Lex 2008/114/EK, 2008) Az irányelv rendelkezik az E-egészségügyről és az egészségügyi technológiák értékelésére vonatkozó együttműködésről a 14. és 15. cikkekben.
- 2014 április 10. Zöld Könyv *a mobil egészségügyről („m-egészségügyről*") (Európai Bizottság, 2014). Az elöregedő lakosság és a krónikus betegségekben szenvedők arányának növekedése egyre jobban megterheli az uniós egészségügyi rendszereket, ennek nyomán pedig nő a kórházi ápolás, valamint a folyamatos gondozás-ápolás aránya, és meredeken emelkednek az egészségügyi ellátás költségei. Az m-egészségügy (mobil egészségügy) az egyik olyan eszközrendszer, mely hozzájárulhat az uniós tagállamok fenntartható egészségügyi rendszereinek biztosításához, a hatékonyabb egészségügyi ellátáshoz. A világpiacon jelenleg több mint 97000 m-egészségügyi alkalmazás érhető el különböző platformokon.

Változatosságuk következtében a fogyasztóknak, a betegeknek vagy az egészségügyi szakembereknek nehéz kiválasztaniuk a legmegfelelőbb m-egészségügyi megoldást vagy alkalmazást a betegbiztonság és az adatok átláthatósága tekintetében. A Zöld Könyv célja — amint azt a 2012–2020 közötti időszakra szóló elektronikus egészségügyi cselekvési terv megfogalmazta — az érdekeltek széles körét összefogó konzultáció indítása, amely az m-egészségügy alkalmazását nehezítő akadályokra, valamint kapcsolódó kérdésekre fókuszál. Így hozzájárul a m-egészségügyben rejlő potenciál kiaknázásához vezető megfelelő módszerek meghatározásához. A Zöld Könyv megvizsgálja a m-egészségügyben rejlő potenciálokat és technológiai szempontokat, majd bemutatja azokat a témákat, melyek tekintetében az érdekelt felek meglátásai szükségesek. Azt is feltárja, hogy a m-egészségügyben milyen lehetőségek rejlenek a betegek egészségének és jóllétének megőrzésére és javítására, valamint pozíciójuk erősítésére.

- 2016. július 6-án került elfogadásra: Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (EUR-Lex 2016/1148, 2016). Az irányelv (NIS irányelv) az első közösségi szintű szabályozás az információbiztonság területén, mely kötelezően és geopolitikai alapon határoz meg szabályokat és kötelező együttműködést egyes intézmények számára. A NIS irányelv előírja az EU-tagállamok számára a rendelkezéseivel harmonizáló stratégiaalkotási kötelezettséget. A 23. cikk felülvizsgálatról rendelkezik. E szerint a Bizottságnak 2019. május 9-ig jelentést kellett benyújtania az Európai Parlamentnek és a Tanácsnak, amelyben értékelték a tagállamok által az alapvető szolgáltatásokat nyújtó szereplők azonosítása során alkalmazott megközelítés következetességét. A Bizottság ezentúl is rendszeresen felülvizsgálja az irányelv működését, és jelentést tesz arról az Európai Parlamentnek és a Tanácsnak. Az irányelv II. mellékletében került megnevezésre az Egészségügyi ágazat. Alágazatként az egészségügyi ellátó létesítmények, mint kiemelten védendő kritikus infrastruktúra elemek. A szervezet típusa szempontjából pedig úgy rendelkezik, hogy: „egészségügyi szolgáltató” minden olyan természetes vagy jogi személy, vagy bármely más jogalany, aki vagy amely jogszerűen nyújt egészségügyi ellátást egy tagállam területén (EUR-Lex 2011/24/EU, 2011).
- 2018. május 25-től kötelező érvényű szabályozás Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) a GDPR. (General Data Protection Regulation) (EUR-Lex 2016/679, 2016). A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok kezelését, védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben

megnőtt. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia hatalmas mértékű fejlődése, a közösségi hálózatok használata, stb. minden eddiginél nagyobb mértékben teszi lehetővé a vállalkozások, közhatalmi szervek, szervezetek számára a személyes adatok felhasználását. A szabályozás a természetes személyek adatkezeléséről, az azzal összefüggő védelemről szóló rendelkezés.

3.2. Főbb hazai jogi szabályzók

Magyarország egyike a 28 tagállamnak, részese a globális fenyegetéseknek, mely az infokommunikációs technológiai robbanás egyik sajátos, sajnálatos velejárója. A kockázatok a hazai egészségügyi informatikai rendszereket, a bennük tárolt adatok feldolgozását és tárolását is érinti. A LÉR egészségügyi ágazathoz is számos jogszabály, rendelet, szabvány kapcsolódók. A meghatározó törvényeket, rendeleteket egy ún. idővonalon tüntettem fel (lásd: *3. ábra*).

3. ábra: **A hazai jogi környezet vonatkozó főbb szabályzói**

Forrás: A szerző saját szerkesztése. Tisóczki (2019)

A technológia, a miniatürizálás fejlődése az alkalmazott hardware és software komponenseknél is hatalmas léptékű változásokat eredményezett. Gondolok itt a mobiltelefóniára, az internetes hálózatok terjedésére, az ezen eszközöket felhasználók többszöröződésére. Ugyanakkor a használathoz kapcsolódó fenyegetettségek is exponenciálisan emelkednek. Többek az elektronikusan kezelt adatok megszerzésére, majd az azokkal történő egyéb műveletek végzésére egyre nagyobb erőforrásokat allokálnak. Ebből következik, hogy a védelemnek is egyre inkább erődödnie kell, az infokommunikációs biztonságot mindinkább fókuszba kell helyeznünk. Hazai és nemzetközi szinten is. A *3. ábra* idővonalán feltüntetett utolsó

piktogram a jövőben megjelenő, előre nem látható fenyegetettségekre adandó válaszokat hivatott ábrázolni.

- 2012. november 12-én törvényt fogadott el az Országgyűlés. Előkészítését a BM OKF végezte, előterjesztője a Belügyminisztérium volt. Az elfogadott törvény kiemelkedik a jogszabályok köréből. A 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Wolters Kluwers, 2012) rendelkezik. E törvény 2. melléklete tartalmazza az egészségügyi ágazatban megtalálható létfontosságú rendszerelemek kijelöléséről szóló részt.
- 2013. október 22-től hatályos a 26/2013. (X.21.) KIM rendelet (NJT 26/2013, 2013), mely az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének szabályairól rendelkezik.
- 2013. márciusában végrehajtási rendelet került kiadásra: A 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról (Wolters Kluwers, 2013). A kormányrendelet rendelkezik a létfontosságú rendszerelemmé történő kijelölésről, valamint a kijelölés visszavonásának szabályairól hazai és uniós létfontosságú rendszerelem esetén. Meghatározza a biztonsági összekötő személy feltételrendszerét. Szól az üzemeltetési biztonsági tervről és horizontális kritériumokról.
- 2013. július 1-től hatályos a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Wolters Kulwers L.tv., 2013). A törvény meghatározza az alapvető elektronikus információbiztonsági követelményeket. Rendelkezik az elektronikus információs rendszerek biztonsági osztályba sorolásáról, az elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintjéről. Meghatározza a törvény hatálya alá tartozó szervezetek elektronikus információs rendszereik védelmét biztosító kötelezettségeit, szól a biztonsági felügyeletről. Információbiztonsági felügyelő kijelöléséről rendelkezik. Bennfoglalja az eseménykezelő központokról, sérülékenységvizsgálatról, kormányzati koordinációról, adatvédelmi rendelkezésekről szóló részeket. A IV. fejezet az oktatás-képzés, kutatás-fejlesztésről szól (Wolters Kulwers L.tv., 2013). Az Országgyűlés két év tapasztalata alapján felülvizsgálta, majd az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról szóló 2015. évi CXXX. törvény elfogadásával módosította az információbiztonsági törvényt, mely 2015. július 16-án lépett hatályba. 2019. január 01-től ismét módosulás következett be. (Lásd alább a 2018. évi CXXI. törvény és 37/2018. (XII. 28.) BM rendeleteket.)
- A 2015 július 16-tól hatályos 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai, biztonsági, valamint a

biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (Wolters Kulwers, 2015), definiálja az információbiztonsági törvény gyakorlati tennivalóit.

- 2015 július: 187/2015. (VII.13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról (NJT 187/2015, 2015). A rendelet szól az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságról, a hatósági eljárásra vonatkozó általános rendelkezésekről, a hatóság feladatairól, regisztrációs eljárásról és hatósági nyilvántartásba vételről. Rendelkezik az érintett szervezeti egység kötelezettségeiről, az ellenőrzési tervről, az információbiztonsági felügyelőről és az egyes jogszabálysértések esetében kiszabható bírság mértékéről is.
- 2015 szeptemberében került kiadásra a 246/2015. (IX. 8.) Korm. Rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (NJT 246/2015, 2015). A jogszabály rendelkezik az ágazati kijelölő hatóságról. Szól a nemzeti létfontosságú rendszerelemek egészségügyi alágazat kritériumairól, valamint az európai létfontosságú rendszerelemek egészségügyi alágazat kritériumairól is. Meghatározza a létfontosságú rendszerelemek azonosítási eljárását. Rendelkezik a biztonsági összekötő személyére vonatkozó szabályokról. Nevesíti a létfontosságú rendszerelemek Üzemeltetői Biztonsági Terveire (ÜBT) vonatkozó különleges szabályokat. Hatályos: 2015. november 25-től.
- 2018-ban került kiadásra a 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről (NJT 270/2018, 2018). A rendelet nem alkalmazható arra a bejelentés-köteles szolgáltatóra, amely kijelölt európai vagy nemzeti létfontosságú rendszerelem. Egyes egészségügyi intézmények WAN kapcsolatainak kiszolgálását biztosító vállalkozások érintettsége miatt azonban szükségét éreztem a rendelet itt történő megemlítését. Ez meghatározza a bejelentés-köteles szolgáltatást nyújtók elektronikus és információs rendszereinek biztonságára vonatkozó alapvető követelményeket, a jelentős biztonsági eseményekkel és azok bejelentésével összefüggő szabályokat. Rendelkezik a jogkövetkezményekről és az egyes jogszabálysértések esetében kiszabható bírságok mértékéről is.
- 2018-ban került elfogadásra és kiadásra a 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól (NJT 271/2018, 2018). A kormányrendelet meghatározza a bejelentési kötelezettségek eseteit,

kezelésület és műszaki vizsgálatainak szabályrendszerét. Rendelkezik a sérülékenység vizsgálatról. A rendelet 2019 január 1-től hatályos.

3.3. Hardware és software környezet

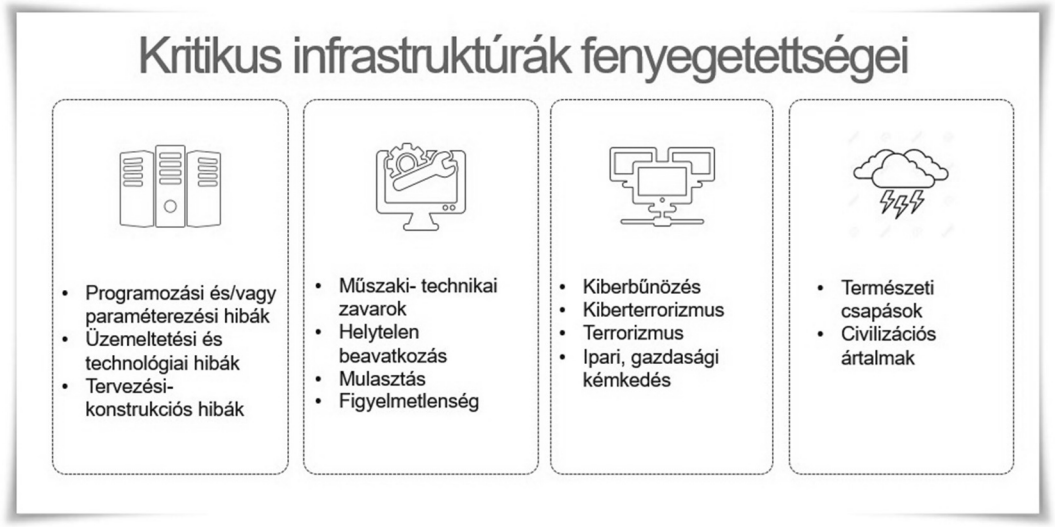
Az egészségügyi ágazat informatikai infrastruktúráinak fejlődésére az ’evolúciós fejlődés’ volt a jellemző kifejezés. A kiépítettséget és felépítettséget a heterogén megoldások jellemezték. Ennek felismerését követően, figyelemmel a hazai egészségügyi ellátók informatikai infrastruktúra megoldásaira, a felmerülő kihívásokra és követelményekre korszerűsítési programok indultak. A szerver és kliens oldali eszköz ellátottság, a hardware erőforrások korszerűsítése jelenleg is zajlik vagy már befejeződött. Regionális, megyei intézmények vonatkozásában a fejlesztések korábban már lezárultak, azok több hazai projekt keretében megvalósultak. Jelenleg kiemelendő a fővárosi kórházakat érintő napjainkban zajló ’Egészséges Budapestért’(EBP) projekt. Keretében a fővárosi betegellátó intézmények teljes informatikai infrastruktúrája is teljesen megújul. „Nagy erőkkel fejlesztik az informatikát: minden kórház IT rendszere meg fog újulni.” (Nyári, 2019)

4. Kihívások, fenyegetettségek az egészségügy IT üzleti folyamataiban

A Magyar egészségügyi intézményrendszer felépítését elképzelhetjük egy öt szintű piramisként is. Az alsó szinten az alapellátás helyezkedik el. Ez magában foglalja a gyermek- és felnőtt háziorvosi ellátást, a fogászati ellátást, az ügyeleti szolgálatokat, az üzemorvosi- és iskolaorvosi ellátást, valamint a védőnői szolgálatot. Következő, második szint a Járóbeteg szakellátás szintje. Itt helyezkednek el a rendelőintézetek, a szakgondozók, a szakambulanciák és a szakápolás. A piramis közepén, harmadik szintjén a városi, megyei ún. általános kórházak találhatóak. E fölött, negyedik szinten a regionális központok jelennek meg. Végül a piramis csúcsa az országos intézetek, egyetemek. Az előzőekben felvázolt összes szinten jelen vannak az IT infrastruktúra működésére irányuló fenyegetettségek (lásd: 4.*ábra*).

A Kormány 1838/2018. (XII. 28.) Korm. határozatban elfogadta Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiáját. A Stratégiában (Kormany.hu, 2018) felsorolt 1–56. pont szerinti intézkedések végrehajtása érdekében a belügyminisztert bízta meg, hogy az érintett miniszterek bevonásával intézkedési tervet készítsen (NJT 1838/2018, 2018). A Stratégiában megfogalmazódik a létfontosságú infrastruktúrákat érintő egyre nagyobb mértékű fenyegetettség. A stratégia részletesen tárgyalja az irányítási keretrendszert, figyelembe véve a védelmi kötelezettségvállalásokat a NATO és az Európai Unió szintjén. Célkitűzéseket és intézkedéseket fogalmaz meg. Többek között célként jelöli meg a bűnüldözés, kiber-bűnüldözés fejlesztését is.

4. ábra: **Létfontosságú rendszerelem (LÉR) fenyegetettségei**



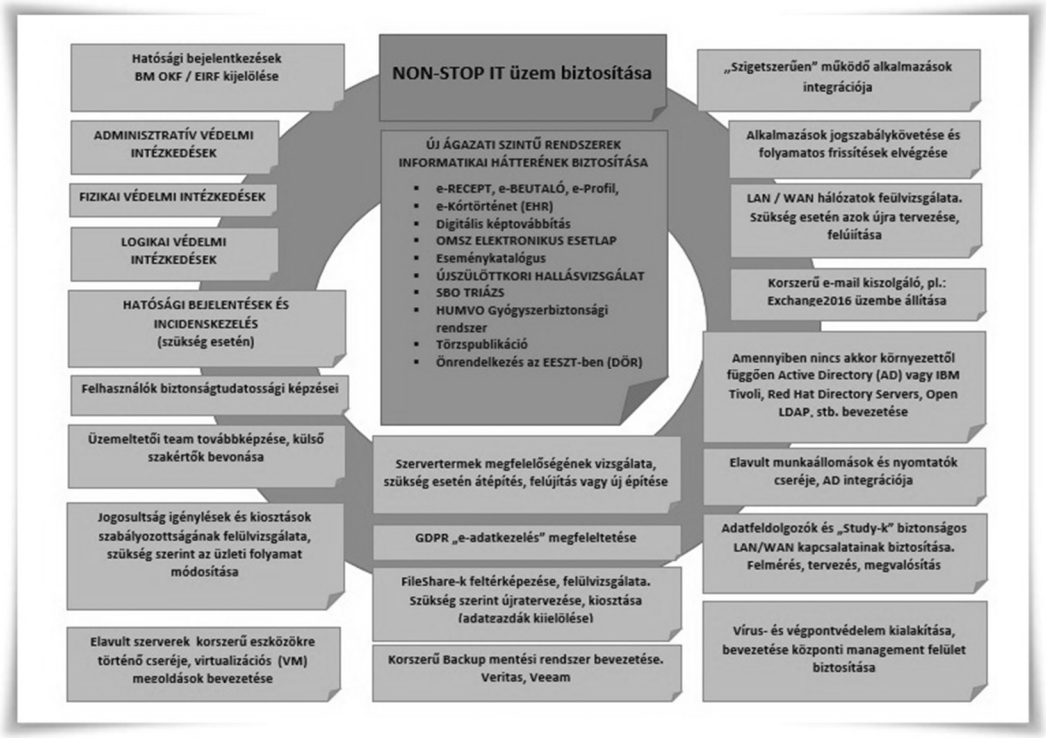
Forrás: Tisóczki (2019)

5. Egészségügyi Elektronikus Szolgáltatások

Az egészségügyi elektronikus szolgáltatások területén 2017 novemberétől bevezetésre került egy új országos platform, melynek elnevezése Elektronikus Egészségügyi Szolgáltatási Tér lett (EESZT). Használata 2017 november 01-től kötelező minden gyógyszertár, háziorvos, állami fenntartású fekvő- és járóbeteg ellátó egészségügyi intézmény számára. 2018. novembertől bekapcsolták az Országos Mentőszolgálatot (OMSZ) és a magán egészségügyi ellátókat is a kötelező platform használatába. Ez a platform kezeli az elektronikus recepteket, beteg életutakra vonatkozó adattartalmakat. Orvos-szakmai oldalról történő hozzáférése kétszintű azonosítást követően valósulhat meg. Az EESZT fejlesztése folyamatosan zajlik. Tervben van a korábbi évekre történő adatfelvitel, adatmigráció elvégzése. Ágazati szinten egy egységesítési folyamat keretében azonos felépítésű űrlapokat kíván az ágazat bevezetni. Tevékenységéhez az OMSZ már 2018 őszétől használja az elektronikus „Esetlapot", a beteg kórház részére történő átadásakor. Tervezés fázisában van a mobil eszközökre történő applikációk fejlesztése, bevezetése ún. „MobilGateWay" elnevezéssel. A technológia és az alkalmazás használata a mobil adatelérést és a mobil adatkezelést fogja segíteni. Óriási jelentőségű lesz a jelenleg kialakítás és bevezetés alatt álló Telemedicina (DKTK) rendszer. Ez a távdiagnosztikát, távleletezést lesz hivatott segíteni. Különféle speciális egészségügyi nyilvántartások a regiszterek. Ezek EESZT-be történő integrálása jelenleg a tervezés fázisában tart, illetve egy-két regiszter on-line használható. Jogszabályokkal körülbástyázott, jól felépített módon történő egészségügyi adatgyűjtés és tárolás, felhasználva a BigData elemzés eszközrendszerét, az egészségpolitikai döntéshozók és az egészségügyi ellátók részére döntéseket magalapozó és ellátást támogató információkat lesz képes szolgáltatni. Napjainkban kialakítás és bevezetés alatt áll a védőnői elektronikus információs rendszer, mely

képes lesz a várandós és gyermek-egészségügyi kiskönyv, gyermek védőoltási napló kezelésére. A 2011.évi CXII. törvény alapján az egészségügyi adatok különleges személyes adatoknak minősülnek. Ezen adatok elektronikus feldolgozása és tárolása során megfelelő védelmet kell biztosítani. Meg kell felelnünk a rendelkezésre állás, a bizalmasság és a sértetlenség hármas követelmény rendszerének. A megfelelőség biztosításához, a non-stop IT üzletmenethez elengedhetetlen, hogy a meglévő rendszereinket felülvizsgáljuk, szükség esetén módosításokat végezzünk (lásd: 5. *ábra*).

5. ábra: **Fenyegetettségekkel összefüggésben végzendő aktuális IT feladatokból**



Forrás: A szerző saját szerkesztése. Tisóczki (2019)

6. Összegzés

A Cybersecurity Ventures felmérése alapján 2019-ben minden 14. másodpercben ramsomware támadás ér egy céget és az áldozattá válik (Cybersecurity Ventures, 2019). Az egészségügyi informatikai rendszereket ért mindennapi kihívásokra válaszként több részelem fejlesztése elengedhetetlenül szükségessé vált. Ezen fejlesztési kihívásokat nem kerülhetjük ki, azokat abszolválnunk kell, hiszen ezek az infrastruktúrák egyre nagyobb szerepet töltenek be életünkben, az állampolgár egészségügyi ellátása során egyre inkább nélkülözhetetlen szolgáltatásról beszélünk. A LÉR alá tartozó egészségügyi intézmények betegadatainak megóvása, a non-stop, biztonságos informatikai üzletmenet közös társadalmi érdekünk. Nem csak a kiberbűnözés jelent kockázatot, számolnunk kell más tényezőkkel is, úgy, mint a

globális időjárásváltozás vagy a felhasználói ismeretek elégtelensége. A jövőben egyre növekvő méretű kockázathalmaz kezelésére kell hatékony megoldásokat találnunk. A jogkövető magatartások és az anyagi ráfordítások mellett is bekövetkeznek incidensek. A védelmi költségek a kockázatok növekedésének és jellegének megfelelően arányosan emelkednek. Teljes mértékű, 100%-os védelem nem építhető, ugyanakkor a teljeshez egyre inkább konvergáló hatékony védelem igen. A hatékony védelem biztosításához az IT üzleti folyamatokban részt vevő minden egyes erőforrás megfontolt, következetes döntése és cselekvése, illetve a gépek algoritmizált cselekvéssorozatának optimális eljárássorozata szükséges. A törvényi szabályzás mellett új, hatékony technológiák bevezetését kell megvalósítanunk az egészségügyi informatikai infrastruktúrákban, a humán erőforrás folyamatos képzése, az infokommunikációs szaktudásuk megújítása mellett.

Irodalomjegyzék

Cybersecurity Ventures (2019): *Infografika.* <https://cybersecurityventures.com/cybercrime-infographic/> (2019.04.12.)

EUR-Lex COM(2006) 786 (2007): *Létfontosságú infrastruktúrák védelmére vonatkozó európai program.* <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Al33260> (2019.04.16.)

EUR-Lex COM(2005) 576 (2005): *COM(2005) 576 végleges Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról.* <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52005DC057> (2019.04.28.)

EUR-Lex 2008/114/EK (2008): *A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javításaszükségességének értékeléséről.* <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32008L0114&from=EN>(2019. 04.15.)

EUR-Lex 2011/24/EU (2011): *Az Európai Parlament és a Tanács 2011/24/EU irányelve (2011. március 9.) a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről.* <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:HU:PDF> (2019.06.01.)

EUR-Lex 2016/679 (2016): *Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).* <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=HU> (2019.04.11.)

EUR-Lex 2016/1148 (2016): *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.* <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148&from=EN> (2019.04.22.)

EUR-Lex 2018/1807 (2018): *Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete (2018. november 14.) a nem személyes adatok Európai Unióban való szabad áramlásának keretéről.* <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32018R1807> (2019.06.02.)

Európai Bizottság (2014): *Zöld Könyv a mobil egészségügyről („m-egészségügyről").* <http://ec.europa.eu/transparency/regdoc/rep/1/2014/HU/1-2014-219-HU-F1-1.Pdf> (2019.04.10.)

European Unio (2018): *A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI)1, Magyarországról szóló országjelentés.* <http://ec.europa.eu/information_society/newsroom/image/document/2018-20/hu-desi_2018-country-profile-lang_4AA43283-EC48-996F-09918493E34A691F_52334.pdf> (2019.05.31)

Fülöp G. (2001): *Az információ*. Erdélyi Múzeum-Egyesület, Kalota Könyvkiadó, Kolozsvár.
Kormany.hu (2018): *A hálózati és információs rendszerek biztonságára vonatkozó Stratégia. (Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján)* <https://www.kormany.hu/download/2/f9/81000/Stratégia honlapon közzétételre-20180103_4829494_2_20190103130721.pdf> (2019.05.02.)
Morris F. Collen (1986): *Origins of Medical Informatics.* In: Medical Informatics [Special Issue]. Oakland, California. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1307150/pdf/westjmed00160-0042.pdf> (2019.04.07.)
NJT 26/2013 (2013): *26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról. Nemzeti Jogszabálytár.* <http://njt.hu/cgi_bin/njt_doc.cgi?docid=164331.250717> (2019.05.05.)
NJT 187/2015 (2015): *187/2015 (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról.* <http://njt.hu/cgi_bin/njt_doc.cgi?docid=176705.363342> (2019.04.02)
NJT 246/2015 (2015): *246/2015 (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.* <http://njt.hu/cgi_bin/njt_doc.cgi?docid=177564.347753> (2019.04.02)
NJT 270/2018 (2018): *270/2018 (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről.* <http://njt.hu/cgi_bin/njt_doc.cgi?docid=211838.362365> (2019.03.04)
NJT 271/2018 (2018): *271/2018 (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól.* <http://njt.hu/cgi_bin/njt_doc.cgi?docid=211839.362368> (2019.03.04)
NJT 1838/2018 (2018): *1838/2018 (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról.* <http://njt.hu/cgi_bin/njt_doc.cgi?docid=212067.363463> (2019.03.26.)
Nyári M. (2019): *Hol is tart az Egészséges Budapest Program? Nagy erőkkel fejlesztik az informatikát: minden kórház IT rendszere meg fog újulni.* <https://hirlevel.egov.hu/2019/02/23/hol-is-tart-az-egeszseges-budapest-program-nagy-erokkel-fejlesztik-az-informatikat-minden-korhaz-it-rendszere-meg-fog-ujulni/> (2019.05.02.)
The USA Patriot Act (2001): *Preserving Life and Liberty* <https://web.archive.org/web/20100102035036/http://www.justice.gov/archive/ll/highlights.htm> (2019.05.10.)
Tisóczki J. (2019): *Létfontosságú rendszerelemként nyilvántartott egészségügyi intézmények jogszabályi környezete.* In: Dr. Keresztes Gábor (szerk.): *Tavaszi Szél – Spring Wind II.* Doktoranduszok Országos Szövetsége, Budapest.
Virányi G. (2012): *A biztonság-fogalomról, másként.* <http://www.pecshor.hu/periodika/XIII/viranyi.pdf> (2019.04.07.)
Wolters Kluwers (2012): *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.* https://net.jogtar.hu/jogszabaly?docid=A1200166.TV. (2019.04.14.)
Wolters Kulwers L.tv. (2013): *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.* <https://net.jogtar.hu/jogszabaly?docid=a1300050.tv> (2019.04.11.)
Wolters Kluwers (2013): *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.* <https://net.jogtar.hu/jogszabaly?docid=A1300065.KOR> (2019.04.14)
Wolters Kulwers (2015): *41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai*

biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. <https://net.jogtar.hu/jogszabaly?docid=a1500041.bm> (2019.02.10.)